

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

ERICA FRASCO, et al. individually and on  
behalf of all others similarly situated,

Plaintiffs,

v.

FLO HEALTH, INC., et al.,

Defendants.

Case No. 3:21-CV-00757-JD

**PROPOSED FINAL JURY  
INSTRUCTIONS**

STIPULATED INSTRUCTION NO. 1:

Members of the jury, now that you have heard all the evidence, it is my duty to instruct you on the law that applies to this case. You will each be given a copy of these instructions to refer to during your deliberations.

All of this means that you must decide the case solely on the evidence before you. Please keep in mind that you took an oath to do so.

**Source:** Google Play Final Instruction No. 1.

STIPULATED INSTRUCTION NO. 2:

MULTIPLE PARTIES

There are two defendants in this trial. You should decide the case against each defendant separately as if it were a separate lawsuit. Each defendant is entitled to separate consideration of that defendant's own defenses.

Different aspects of this case involve different parties (plaintiffs and defendants). Each instruction will identify the parties to whom it applies. Pay particular attention to the parties named in each instruction.

***Source:*** CACI No. 103.



1 exactly what it told users it would do. (2) Even without those disclosures, the use of performance  
2 SDKs is routine in the App industry. Users do not have a reasonable expectation that apps will not  
3 use such tools, and the use of standard tools used by nearly all apps is not the kind of “highly  
4 offensive” conduct that can support a legal claim for invasion of privacy. (3) The custom app events  
5 are not medical information nor are they personally identifiable. Flo did not reveal users’ actual  
6 inputs into the App or answers to the first launch questions but only data about where a device  
7 navigated within the App. Moreover, this information was not linked to any names, dates of birth,  
8 emails, or contact information but only to de-identified device information. And (4) Flo did not  
9 violate the Confidentiality of Medical Information Act, which protects actual medical records  
10 created by doctors, because Flo is not a provider of healthcare, Plaintiffs are not Flo’s patients, and  
11 Flo’s use of SDKs was authorized by Plaintiffs and by the law.

12 Flo also asserts two affirmative defenses against Plaintiffs’ claims. First, Flo claims that  
13 users consented to its use of SDKs and the alleged sharing of custom app events, all of which were  
14 clearly disclosed in Flo’s Privacy Policy, which users affirmatively agreed to before using the App.  
15 Second, Flo alleges that Plaintiffs did not file their lawsuit within the one-year time limit set by law.  
16 In fact, Flo always disclosed its use of SDKs to users through its Privacy Policy, including  
17 specifically identifying Facebook by name in its very first Privacy Policy in 2016. And Flo’s use of  
18 SDKs became nationwide news in February 2019. Nevertheless, Plaintiffs waited until 2021 to file  
19 this lawsuit. Flo has the burden of proving these affirmative defenses.

20 **Defendant Meta’s Statement:**

21 Meta denies Plaintiffs Chen, Gamino, and Wellman’s claim. Meta contends that: (1) Meta  
22 did not receive Plaintiffs’ communications with Flo, let alone eavesdrop on or record them; (2) Meta  
23 only received limited, coded information that Flo sent; (3) Meta never intended to receive (and  
24 believes it did not receive) confidential communications; (4) if Meta inadvertently received any  
25 confidential communications, any receipt was against the Terms of Use for Meta’s SDK and not  
26 intentional; and (5) any data Meta received was transmitted with these Plaintiffs’ and Flo’s consent.  
27  
28

1           Meta asserts one affirmative defense against Plaintiffs Chen, Gamino, and Wellman's claim.  
2           Meta alleges that these Plaintiffs did not file their lawsuit within the time set by law. Meta has the  
3           burden of proving this affirmative defense.  
4

5  
6           **Source:** Google Play Final Instruction No. 2.  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

STIPULATED INSTRUCTION NO. 4:

CORPORATIONS -- FAIR TREATMENT

The Defendants in this case are corporations. All parties are equal before the law and a corporation is entitled to the same fair and conscientious consideration by you as any party.

Under the law, a corporation is considered to be a person. It can only act through its employees, agents, directors, or officers. Therefore, a corporation is responsible for the acts of its employees, agents, directors, and officers, performed within the scope of authority. An act is within the scope of a person's authority if it is within the range of reasonable and foreseeable activities that an employee, agent, director, or officer engages in while carrying out that person's business.

**Source:** Google Play Final Instruction No. 3.

STIPULATED INSTRUCTION NO. 5:

WHAT IS EVIDENCE

The evidence you are to consider in deciding what the facts are consists of:

1. the sworn testimony of any witness;
2. the exhibits that are admitted into evidence;
3. any facts to which the lawyers have agreed; and
4. any facts that I may instruct you to accept as proved.

**Source:** Google Play Final Instruction No. 4.



STIPULATED INSTRUCTION NO. 6:

## WHAT IS NOT EVIDENCE

In reaching your verdict, you may consider only the testimony and exhibits received into evidence, any facts to which the lawyers have agreed, and any facts that I may instruct you to accept as proved. Certain things are not evidence, and you may not consider them in deciding what the facts are. I will list them for you:

1. Arguments and statements by lawyers are not evidence. The lawyers are not witnesses. What they have said in their opening statements, closing arguments, and at other times is intended to help you interpret the evidence, but it is not evidence. If the facts as you remember them differ from the way the lawyers have stated them, your memory of them controls.

2. Questions and objections by lawyers are not evidence. Attorneys have a duty to their clients to object when they believe a question is improper under the rules of evidence. You should not be influenced by the objection or by the Court's ruling on it.

3. Testimony that was excluded or stricken, or that you have been instructed to disregard, is not evidence and must not be considered. In addition, some evidence was received only for a limited purpose; when I have instructed you to consider certain evidence only for a limited purpose, you must do so, and you may not consider that evidence for any other purpose.

4. Anything you may have seen or heard when the Court was not in session is not evidence. You are to decide the case solely on the evidence received at the trial.

**Source:** Google Play Final Instruction No. 5.

STIPULATED INSTRUCTION NO. 7:

DIRECT AND CIRCUMSTANTIAL EVIDENCE

Evidence may be direct or circumstantial. Direct evidence is direct proof of a fact, such as testimony by a witness about what that witness personally saw or heard or did. Circumstantial evidence is proof of one or more facts from which you could find another fact. You should consider both kinds of evidence. The law makes no distinction between the weight to be given to either direct or circumstantial evidence. It is for you to decide how much weight to give to any evidence.

**Source:** Google Play Final Instruction No. 6.

STIPULATED INSTRUCTION NO. 8:

RULING ON OBJECTIONS

There are rules of evidence that control what can be received into evidence. When a lawyer asked a question or offered an exhibit into evidence and a lawyer on the other side thought that it was not permitted by the rules of evidence, that lawyer objected. If I overruled the objection, the question was answered, or the exhibit received. If I sustained the objection, the question was not answered, or the exhibit was not received. Whenever I sustained an objection to a question, you must ignore the question and must not guess what the answer might have been.

Sometimes I ordered that you disregard or ignore that evidence. That means that when you are deciding the case, you must not consider the stricken evidence for any purpose.

**Source:** Google Play Final Instruction No. 7.

STIPULATED INSTRUCTION NO. 9:

DEPOSITION IN LIEU OF LIVE TESTIMONY

During the trial, you heard testimony by witnesses in the form of previously recorded trial and deposition testimony, rather than live here in court. A deposition is the sworn testimony of a witness taken before trial. The witness was placed under oath to tell the truth, and lawyers for each side asked questions. The questions and answers were recorded.

Insofar as possible, you should consider deposition testimony presented to you in court in lieu of live testimony, in the same way as if the witnesses had been present to testify.

**Source:** Google Play Final Instruction No. 8.

## STIPULATED INSTRUCTION NO. 10:

## CREDIBILITY OF WITNESSES

In deciding the facts in this case, you may have to decide which testimony to believe and which testimony not to believe. You may believe everything a witness said, or part of it, or none of it.

In considering the testimony of any witness, you may take into account:

1. the opportunity and ability of the witness to see or hear or know the things testified to;
2. the witness's memory;
3. the witness's manner while testifying;
4. the witness's interest in the outcome of the case, if any;
5. the witness's bias or prejudice, if any;
6. whether other evidence contradicted the witness's testimony;
7. the reasonableness of the witness's testimony in light of all the evidence; and
8. any other factors that bear on believability.

Sometimes a witness may have said something that is not consistent with something else he or she said. Sometimes different witnesses gave different versions of what happened. People often forget things or make mistakes in what they remember. Also, two people may see the same event but remember it differently. You may consider these differences, but do not decide that testimony is untrue just because it differs from other testimony.

However, if you decide that a witness has deliberately testified untruthfully about something important, you may choose not to believe anything that witness said. On the other hand, if you think the witness testified untruthfully about some things but told the truth about others, you may accept the part you think is true and ignore the rest.

The weight of the evidence as to a fact does not necessarily depend on the number of witnesses who testify. What is important is how believable the witnesses were, and how much weight you think their testimony deserves.

**Source:** Google Play Final Instruction No. 9.

STIPULATED INSTRUCTION NO. 11:

EXPERT OPINION

You have heard testimony from expert witnesses who testified to opinions and the reasons for their opinions. This opinion testimony was allowed because of the education or experience of the expert witness.

Such opinion testimony should be judged like any other testimony. You may accept it, reject it, or give it as much weight as you think it deserves, considering the witness's education and experience, the reasons given for the opinion, and all the other evidence in the case.

**Source:** Google Play Final Instruction No. 10.



STIPULATED INSTRUCTION NO. 13:

STIPULATIONS OF FACT

The parties have agreed to certain facts that I will now read to you. You must treat these facts as having been proved.

1. Plaintiff Erica Frasco is a citizen of the State of New Jersey who downloaded the Flo App.

2. Plaintiff Sarah Wellman is a citizen of the State of California who downloaded the Flo App.

3. Plaintiff Jennifer Chen is a citizen of the State of California who downloaded the Flo App.

4. Plaintiff Tesha Gamino is a citizen of the State of California who downloaded the Flo App.

5. Plaintiff Autumn Meigs is a citizen of the State of Ohio who downloaded the Flo App.

6. Defendant Flo Health, Inc. ("Flo") is the developer of the Flo App.

7. Defendant Meta Platforms, Inc., ("Meta") is a technology company that, among other things, offers free tools like the SDK that allow businesses to build unique and customized solutions to serve their clients.

8. Plaintiffs first filed a lawsuit against Flo based on purported injuries arising from their use of the Flo App on January 29, 2021.

9. Plaintiffs first filed a lawsuit against Meta based on purported injuries arising from their use of the Flo App on June 7, 2021.

10. Flo was created in 2015 and launched the Flo App in 2016.

11. During the Class Period, the Flo App was available for download on the iOS and Android app stores.

12. The Flo App is a mobile application that can be used to track periods and pregnancy.



1           13. Plaintiffs Chen, Frasco, Gamino, and Meigs downloaded the Flo App to track their  
2 menstrual cycles. Plaintiff Wellman downloaded the Flo App to track her menstrual activity and  
3 figure out the best day to get pregnant.

4           14. During the Class Period, Meta offered SDKs to app developers.

5           15. Flo incorporated code from the Facebook SDK into the Flo App throughout the Class  
6 Period.

7           16. Flo incorporated the Fabric SDK into the Flo App prior to the deprecation of Fabric  
8 in 2020.

9           17. The Custom App Event names at issue in this lawsuit are:

- 10           • “R\_CHOOSE\_GOAL”;
- 11           • “R\_SELECT\_LAST\_PERIOD\_DATE”;
- 12           • “R\_SELECT\_CYCLE\_LENGTH”;
- 13           • “R\_SELECT\_PERIOD\_LENGTH”;
- 14           • “R\_AGE\_CHOSEN\_PERIODS”;
- 15           • “R\_AGE\_CHOSEN\_PREGNANCY”;
- 16           • “R\_AGE\_CHOSEN\_PREGNANCY\_METHOD”;
- 17           • “R\_PREGNANCY\_METHOD”;
- 18           • “R\_PREGNANCY\_METHOD\_DATE”;
- 19           • “R\_PREGNANCY\_WEEK\_CHOSEN”;
- 20           • “R\_PREGNANCY\_WEEK\_CHOSEN\_UNKNOWN”;
- 21           • “SESSION\_CYCLE\_DAY”

22           18. Flo shared the Custom App Events I just read to you with Meta.

23  
24 **Sources:** Google Play Final Instruction No. 12; Joint Pretrial Statement Regarding June 26, 2025  
25 Pretrial Conference, Section III (Undisputed Facts), ECF No. 656.

STIPULATED INSTRUCTION NO. 14:

BURDEN OF PROOF -- PREPONDERANCE OF THE EVIDENCE

When a party has the burden of proving any claim or affirmative defense by a preponderance of the evidence, it means you must be persuaded by the evidence that the claim or affirmative defense is more probably true than not true.

You should base your decision on all of the evidence, regardless of which party presented it.

**Source:** Google Play Final Instruction No. 14.

DISPUTED INSTRUCTION NO. 15:

ELEMENTS OF PLAINTIFFS' CLAIM FOR VIOLATION OF CALIFORNIA  
CONFIDENTIALITY OF MEDICAL INFORMATION ACT, Cal. Civ. Code §§ 56 et seq  
("CMIA") AGAINST FLO HEALTH  
**OFFERED BY PLAINTIFFS**

Plaintiffs, as Class Representatives, assert that Flo violated the CMIA.

To establish this claim, Plaintiffs, as Class Representatives, must prove, by a preponderance of the evidence:

1. That Flo is a healthcare provider. Under the CMIA Flo is a healthcare provider if they are a business that is:

a. organized for the purpose of maintaining medical information in order to make the information available to an individual, or a provider of healthcare, at the request of the individual or a provider of health care, for the purposes of allowing the individual to manage their information or for diagnosis and treatment of the individual;

OR

b. that offers software to consumers, including a mobile application, that is designed to maintain medical information in order to make the information available to an individual, or a provider of health care, at the request of the individual or a provider of health care, for purposes of allowing the individual to manage their health information or for diagnosis, treatment, or management of a medical condition.

2. Plaintiffs, as Class Representatives, must also prove, by a preponderance of the evidence:

1 That Flo disclosed Plaintiffs' and Class Members' medical information without  
2 authorization. For purposes of this claim, "medical information" means individually identifiable  
3 information relating to an individual's medical history, mental or physical condition, or treatment.  
4 Information is "individually identifiable" if it contains any element of personally identifying  
5 information sufficient to allow identification of the individual or other information that, when  
6 combined with other publicly available information, reveals the individual's identity.  
7

8 3. Plaintiffs and Class Members need not show that they suffered harm as a result of the  
9 disclosure to prove a violation of the CMIA.  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

***Plaintiffs’ Position:***

No model instruction exists for the CMIA. Cal. Civ. Code §§ 56 *et seq.* As explained below, Plaintiffs’ proposal correctly tracks the statutory text that was operative during the Class Period, and is entirely consistent with the Court’s rulings throughout this case. In contrast, Flo’s competing position is inconsistent with the statute and merely seeks to relitigate meritless legal positions they previously raised and lost at earlier stages in the case. The parties’ disputed views, here, reflect a critical and **fundamental disagreement** that requires resolution by the Court.

At all relevant times, the CMIA stated that: “a provider of health care . . . shall not disclose medical information regarding a patient of the provider of health care . . . without first obtaining an authorization.” *Id.* §§ 56.10 (statute effective from January 1, 2017 to the present). This is the operative text giving rise to Plaintiffs’ CMIA claims, and it uses three relevant defined terms:

- Section 56.05(p) initially defines “**provider of healthcare**,” and § 56.06 expands this definition under the heading “Businesses deemed to be provider of healthcare subject to the requirements of [the] [CMIA].” Specifically, throughout the Class Period, Section 56.06 defined “provider of healthcare” using the same text Plaintiffs include in ¶ 1 of their proposed instruction.

- Throughout the Class Period, § 56.05(j) defined “**patient**” as one “who received health care services from a provider of health care and to whom medical information pertains.”

- Throughout the Class Period, § 56.05(p) defined “**medical information**,” as stated in ¶ 2 of Plaintiffs’ proposed instruction, to mean “any individually identifiable information<sup>1</sup> . . . in possession of or derived from a provider of health care . . . regarding a patient’s medical history, mental or physical condition or treatment.”

Thus, Plaintiffs’ proposal mirrors the applicable statutory text. Moreover, Plaintiffs’ proposal also closely mirrors the Court’s prior rulings concerning the application of the CMIA in this case, which independently justifies Plaintiffs’ proposal as it tracks the law of the case. *See Gonzalez v. Arizona*, 677 F.3d 383, 389 n.4 (9th Cir. 2012), *aff’d sub nom. Arizona v. Inter Tribal*

---

<sup>1</sup> The CMIA defines “individually identifiable” as information includes “any element of personal identifying information sufficient to allow identification of the individual, such as [their] name . . . telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual’s identity.” CMIA § 56.05(j).

1 *Council of Arizona, Inc.*, 570 U.S. 1 (2013) (“Under the law of the case doctrine, a court will  
 2 generally refuse to reconsider an issue that has already been decided by the same court or a higher  
 3 court in the same case.”).<sup>2</sup> Additionally, Plaintiffs’ proposal is also consistent with prior cases  
 4 interpreting the CMIA. *E.g.*, *J.M. v. Illuminate Educ., Inc.*, 103 Cal. App. 5th 1125, 1131 (Cal. Ct.  
 5 App. 2024) (reasoning that § 56.06(b) applies to an “education company” that uses software to  
 6 “store[]” “mental health” information to provide “assistance” and “diagnose” student “needs”).

7 In contrast, Flo improperly attempts to relitigate legal issues the Court has already resolved.  
 8 Flo may be unhappy with the Court’s prior rulings, but a jury charging conference is not the time to  
 9 move for reconsideration—that time has long since passed, and the law of the case doctrine exists  
 10 specifically to prevent this kind of repetitive litigation. *See Gonzalez*, 677 F.3d at 389 n.4.

11 Specifically, Flo’s proposed instruction essentially repeats its arguments that it is not subject  
 12 to the CMIA—a position this Court has already rejected twice. First, in denying Flo’s motion to  
 13 dismiss, the court implicitly rejected Flo’s arguments that the CMIA was inapplicable. ECF No.  
 14 158. Indeed, Flo moved to dismiss Plaintiffs’ CMIA claim, arguing that Flo doesn’t qualify as a  
 15 “provider of healthcare” under the statute, user inputs are not “medical information . . . derived from  
 16 a provider of health care” because users self-reported the data, and “Plaintiffs did not rely on doctors  
 17 to tell them when they were menstruating.” ECF No. 93 at 14. The Court rejected these arguments  
 18 when it upheld Plaintiffs’ CMIA claims.

19 Second, the Court denied Flo’s Motion for Summary Judgment (ECF No. 608) on Plaintiffs’  
 20 CMIA claim, stating, “Flo’s arguments are not well taken.” *Id.* at 3. The Court rejected Flo’s  
 21 arguments that: (i) it was not a “provider of healthcare,” (ii) the “CMIA did not apply to” women’s  
 22 health apps, and (iii) the data was “de-identified” and thus not “medical information.” *Id.* at 3-4.  
 23 The Court also specifically addressed and rejected Flo’s argument that the CMIA “did not apply to  
 24 pregnancy and fertility tracker apps like Flo from 2016 through 2019.” *Id.*

25  
 26 <sup>2</sup> In the Ninth Circuit, the only exceptions to the law of the case doctrine—which are not even  
 27 arguably applicable here—are: “(1) the decision is clearly erroneous and its enforcement would  
 28 work a manifest injustice, (2) intervening controlling authority makes reconsideration appropriate,  
 or (3) substantially different evidence was adduced at a subsequent trial.” *Gonzalez*, 677 F.3d at  
 389 n.4; *see also United States v. Gartenlaub*, 2024 WL 4987258, at \*1 (9th Cir. Dec. 5, 2024)  
 (noting that “the law of the case doctrine has only three exceptions,” citing *Gonzalez*).

1           Nonetheless, through its proposed instruction, Flo continues to argue that it is not bound by  
 2           the CMIA because, prior to January 1, 2024, the CMIA did not expressly reference “reproductive or  
 3           sexual health digital service[s].” *See* § 56.05(r) (2024). As noted, the Court already considered and  
 4           rejected this argument. *See* ECF No. 608 at 3-4.<sup>3</sup> Moreover, this argument is a red herring, as  
 5           Plaintiffs’ proposed instruction does not mention “reproductive or sexual health digital service[s],”  
 6           rather it uses the text of the statute as it existed throughout the Class Period.

7           Flo’s proposed instruction improperly defines “Provider of Healthcare” as exclusively tied  
 8           to information originating from a medical doctor or hospital etc. Flo reaches this conclusion by  
 9           essentially ignoring the express text of CMIA § 56.06, which offers a much broader definition.  
 10          Accepting Flo’s proposal would essentially read § 56.06 out of the statute. As stated above, Flo’s  
 11          argument is inconsistent with the Court’s prior rulings and prior case law.

12          Under Flo’s proposed instruction, the jury could never find Flo qualifies as a provider of  
 13          health care because Flo is not a doctor or hospital, etc. and collects information directly from users.  
 14          That would effectively direct a verdict in its favor by making it legally impossible for the jury to  
 15          find CMIA liability and nullify the Court’s summary judgment ruling.

16          Flo’s proposed instruction should be rejected as legally erroneous and as an improper attempt  
 17          to relitigate legal questions the Court already resolved.

18  
19  
20  
21  
22  
23  
24  
25  
26          <sup>3</sup> The amendment Flo points to was merely a clarifying change responding to heightened privacy  
 27          concerns after the Supreme Court’s decision in *Dobbs v. Jackson Women’s Health Org.*, 597 U.S.  
 28          215 (2022) (overturning *Roe v. Wade*), which is shown by the timing of the amendment immediately  
 after *Dobbs* created new privacy risks for reproductive health data, and the fact that (as the Court  
 previously held) § 56.06(b) of the CMIA already covered health apps maintaining medical  
 information. The amendment reflects the California legislature’s intention to eliminate any doubt  
 in the post-*Dobbs* era, not an admission that such apps were not already covered.

DISPUTED INSTRUCTION NO. 15:ELEMENTS OF PLAINTIFFS' CLAIM FOR VIOLATION OF CALIFORNIA  
CONFIDENTIALITY OF MEDICAL INFORMATION ACT AGAINST FLO**OFFERED BY FLO**

Plaintiffs assert that Flo violated the California Confidentiality of Medical Information Act ("CMIA"). To establish this claim, Plaintiffs, as Class Representatives, must prove, by a preponderance of the evidence:

1. That Flo is a provider of healthcare or can be deemed to be a provider of healthcare. This requires them to prove that from November 2016 through February 2019 Flo:

a. was a provider of health care, meaning a licensed and registered medical doctor, osteopath, medical clinic, health dispensary, or health clinic or hospital

OR

b. was a business organized for the purpose of maintaining medical information that is in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, where "provider of healthcare" means a licensed and registered medical doctor, osteopath, medical clinic, health dispensary, or health clinic or hospital AND maintains that information for the purpose of (i) allowing the individual to manage his or her information, or (ii) for the diagnosis, treatment, or management of a medical condition;

OR

c. offered software or hardware that was designed to maintain information that is in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, where "provider of healthcare" means a licensed and registered medical doctor, osteopath, medical clinic, health dispensary, or health clinic or hospital AND that the App's purpose is to make the information available to an individual or a provider of health care for purposes of (i) allowing the individual to manage his or her information, or (ii) for the diagnosis, treatment, or management of a medical condition;



AND, all of the following:

2. That Plaintiffs are Flo’s “patients,” meaning that they received medical services from Flo;

AND

3. That Flo disclosed Plaintiffs’ medical information without authorization;

AND

4. That the information disclosed by Flo is “medical information,” meaning information regarding Plaintiffs’ medical history, mental or physical condition, or treatment;

AND

5. The medical information disclosed by Flo was individually identifiable.

AND

6. That an unauthorized person actually viewed the alleged medical information.

“Individually identifiable” means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient’s name, address, electronic mail address, telephone number, or social security number, or other information that, when combined with other publicly available information, reveals the identity of the individual.

A CMIA violation only occurs if the disclosure was “unauthorized.” Flo’s disclosure of alleged medical authorization was “authorized”—and therefore Flo did not violate the CMIA—if any of the following is true:

1. Plaintiffs consented to the disclosure;

OR

2. Meta provides data processing or other administrative services to Flo;

OR

3. The disclosure was made for purposes of encoding, encrypting, or otherwise anonymizing data.

**Source:** California Civil Code § 56.05(k), (j), (m) (2014-21); *id.* § 56.06(b) (2015); *id.* §§ 56.10(a), (b)(3), (b)(16) (2017).

**Defendant Flo's Position:**

No CACI or Ninth Circuit Model Instruction exists for the CMIA. However, Flo submits this jury instruction as it is consistent with the California Medical Information Act ("CMIA") that was in effect during the Class Period because it tracks the statutory language and controlling California case law verbatim to the greatest extent possible.

By contrast, Plaintiffs' proposed instructions omit key elements required by the CMIA.

First, the CMIA distinguishes between actual providers of healthcare and entities that are only "deemed to be a provider of health care subject to the requirements of [the CMIA]" because they maintain medical information (or provide software to maintain medical information) for enumerated purposes. *Id.* § 56.06(a)-(b). Plaintiffs' proposed instruction collapses this distinction and creates a false impression that California law considers apps to be actual healthcare providers.

Second, the definition of "medical information" explicitly states that medical information must be "in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment." Cal. Civ. Code § 56.05(j) (2014 version). The statute also defines "Provider of Healthcare" to mean, in essence, doctors and hospital. *Id.* § 56.05. This should be part of the instruction on the definition of "medical information." Plaintiffs' proposal reads this definition out of Cal. Civ. Code § 56.05(j).

Third, during the relevant timeframe the provisions of § 56.06(a)-(b) that deem certain companies to be healthcare providers subject to the CMIA applied only to companies that "maintain[] medical information, *as defined in subdivision (j) of Section 56.05.*" Civ. Code § 56.06(a) & (b) (2018 version) (emphasis added) (the 2014 version in effect at the beginning of the class period contained analogous language). In other words, the information maintained by Flo must be "medical information" in its own right—including the requirement that it be created by an actual provider of healthcare—*before* Flo receives it. For example, these provisions might apply to an app offered by an HMO to allow users to view their medical records, not to apps like Flo's that collect only self-reported information by lay users. Plaintiffs' draft draws on post-class period versions of the statute that omit the cross reference to § 56.05(j).

Nor can Plaintiffs sidestep this issue by invoking Cal. Civ. Code § 56.06, which “deems” certain entities to be “provider[s] of health care *subject to the requirements of this part.*” Cal. Civ. Code § 56.06(a), (b). While those provisions require developers of certain apps (but not fertility trackers like Flo) to adhere to the requirements of the CMIA, it does nothing to change the definition of “medical information,” which is clearly set forth in § 56.05(j).

Fourth, Plaintiffs’ proposed instructions ignores that Flo must have disclosed information “regarding a patient of the provider of healthcare” (i.e., Flo). Civ. Code § 56.10(a) (2017 version). The CMIA explicitly defines the term “patient”: “‘Patient’ means any natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains.” *Id.* § 56.05(k). The CMIA does not prohibit even healthcare providers from disclosing information unless that information is about their patients.

Fifth, the California Court of Appeals has repeatedly and consistently held that an unauthorized disclosure only occurs if the medical information was “actually viewed” by an unauthorized person. *Sutter Health v. Superior Ct.*, 227 Cal. App. 4th 1546, 1555, 174 Cal. Rptr. 3d 653, 659 (2014); *Regents of Univ. of California v. Superior Ct.*, 220 Cal. App. 4th 549, 570, 163 Cal. Rptr. 3d 205, 221 (2013). Merely allowing an unauthorized person to *obtain* medical information, absent proof that person actually viewed the information, is insufficient to sustain a CMIA claim. *Sutter Health*, 227 Cal. App. 4th at 1555.

Plaintiffs’ arguments misstate Flo’s position and the Court’s prior rulings. Contrary to Plaintiffs’ characterization, the Court has not ruled in their favor on any of these issues because Plaintiffs never moved for summary judgment. The denial of Flo’s motion for summary judgment is not a finding in Plaintiffs’ favor. It is “well established that issue finding rather than issue determination is the pivot upon which the summary judgment law turns.” *Walsh v. Walsh*, 18 Cal. 2d 439, 441 (1941). “A motion for summary judgment is not a trial upon the merits. It is merely to determine whether there is an issue to be tried.” *Id.* (quoting *Shea v. Leonis*, 29 Cal. App. 2d 184, 187). Rather, the Court explicitly held that whether Flo is a provider of healthcare and whether the information at issue is CMIA medical information are questions for the jury. ECF No. 608 at 3-4.

Likewise, Flo is not seeking to relitigate these issues via jury instructions. Rather, since these are questions that the Court has left for the jury, Flo has provided instructions on what the jury must find that are taken verbatim from the relevant statutory provisions of the CMIA.

**Reference source as to definition of “Medical Information” Cal. Civ. Code § 56.05(j) (2014 version)**

“Medical information” means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. “Individually identifiable” means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.

**Reference source as to definition of “Patient” Cal. Civ. Code § 56.05(k) (2014 version)**

(k) “Patient” means any natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains.

**Reference source as to definition of “Provider of Health Care” Cal. Civ. Code § 56.05(m) (2014 version)**

(m) “Provider of health care” means any person licensed or certified pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code; any person licensed pursuant to the Osteopathic Initiative Act or the Chiropractic Initiative Act; any person certified pursuant to Division 2.5 (commencing with Section 1797) of the Health and Safety Code; any clinic, health dispensary, or health facility licensed pursuant to Division 2 (commencing with Section 1200) of the Health and Safety Code. “Provider of health care” does not include insurance institutions as defined in subdivision (k) of Section 791.02 of the Insurance Code.

**Reference source as to entities deemed to be provider subject to the CMIA Cal. Civ. Code § 56.06(a) & (b) (2018 version)**

(a) Any business organized for the purpose of maintaining medical information, as defined in subdivision (j) of Section 56.05, in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis and treatment of the individual, shall be deemed to be a provider of health care subject to the requirements of this part. However, this section shall not be construed to make a business specified in this subdivision a

**Reference source as to elements of an unauthorized disclosure. Cal. Civ. Code § 56.10(a) (2017 version)**

**Reference source as to authorization requirement and disclosures that do not require patient authorization. Civ. Code § 56.10(a) & (c) (2017 version)**

(c) A provider of health care or a health care service plan may disclose medical information as follows:

(3) The information may be disclosed to a person or entity that provides billing, claims management, medical data processing, or other administrative services for providers of health care or health care service plans or for any of the persons or entities specified in paragraph (2). However, information so disclosed shall not be further disclosed by the recipient in a way that would violate this part.

PROPOSED FINAL JURY INSTRUCTIONS  
Case No. 3:21-CV-00757-JD

1       (16) The information may be disclosed to a third party for purposes of encoding, encrypting, or  
2       otherwise anonymizing data. However, no information so disclosed shall be further disclosed by  
3       the recipient in a way that would violate this part, including the unauthorized manipulation of  
4       coded or encrypted medical information that reveals individually identifiable medical information.  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

DISPUTED INSTRUCTION NO. 16

## DEFINITION OF “AUTHORIZATION” UNDER THE CMIA

**OFFERED BY PLAINTIFFS**

The CMIA sets forth the following requirements for determining whether the disclosure of information was authorized. An authorization is only valid if it is provided in a document:

(i) that is handwritten or typed in a document with at least 14-point font;

AND

(ii) is clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization;

AND

(iii) stated the specific uses and limitations on the types of medical information to be disclosed;

AND

(iv) stated the name or functions of the provider of health care, health care service plan, pharmaceutical company, or contractor that may disclose the medical information;

AND

(v) stated the name or functions of the persons or entities authorized to receive the medical information;

AND

(vi) stated the specific uses and limitations on the use of the medical information by the persons or entities authorized to receive the medical information;

AND

(vii) stated a date or event upon which the authorization expires;

AND

(viii) advised the person signing the authorization of the right to receive a copy of the authorization.

1 ***Plaintiffs' Position:***

2 No model instruction exists for the CMIA. Cal. Civ. Code §§ 56 *et seq.* This instruction is  
3 necessary because the CMIA's statutory definition of authorization is essential to its statutory  
4 regime. Plaintiffs' proposed instruction closely tracks the language the CMIA uses to define  
5 authorization. CMIA § 56.11.  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28



**OFFERED BY FLO**

To establish their claim, Plaintiffs, as Class Representatives, must prove, by a preponderance of the evidence that Flo's alleged disclosure of medical information was unauthorized. You must find that the disclosure was authorized if you conclude that any of the following are true:

1. Plaintiffs consented to the disclosure;

OR

2. Meta and Google provide data processing or other administrative services to Flo;

OR

3. The disclosure was made for purposes of encoding, encrypting, or otherwise anonymizing data.

**Source:** California Civil Code §§ 56.10(a), (b)(3), (b)(16) (2017 version)

**Defendant Flo's Position:**

No CACI exists for the CMIA, and Flo agrees that the jury should be instructed on what constitutes an authorized or unauthorized disclosure. As indicated above, Flo believes this can be done as part of the general instruction on CMIA. However, if given as a separate instruction, it should be given in the form provided by Flo here.

Cal. Civ. Code § 56.11 is inapplicable to this case. Unauthorized disclosures are governed by § 56.10, which provides that disclosure is permitted where there is (1) “an authorization” or (2) the disclosure falls within certain enumerated exceptions. By contrast, § 56.11 sets out authorization required for recipients to obtain information from healthcare providers, not for health care providers to disclose it. Cal. Civ. Code § 56.11. That provision reads: “Any person or entity *that wishes to obtain* medical information pursuant to subdivision (a) of Section 56.10, other than a person or entity authorized to receive medical information pursuant to subdivision (b) or (c) of Section 56.10, except as provided in paragraph (21) of subdivision (c) of Section 56.10, shall obtain a valid authorization for the release of this information.” *Id.* (emphasis added). Moreover, applying this requirement to the alleged disclosure by an app would lead to an absurd result whereby apps would be required to obtain hand-written medical releases from millions of users. In addition, Plaintiffs’ proposed instruction

Furthermore, Plaintiffs’ proposal ignores that direct consent by the patient is not the only means by which a disclosure can be “authorized.” Cal. Civ. Code § 56.10 also permits (or requires) disclosure without patient consent in dozens of enumerated circumstances. As relevant here, the CMIA does not prohibit disclosures to entities “that provide[] billing, claims management, medical *data processing, or other administrative services for providers of health care*” or where the disclosure is made “to a third party for purposes of encoding, encrypting, or otherwise anonymizing data.” Cal. Civ. Code § 56.10(c)(3) & (16). Both of these circumstances are present here because

1 Meta and Google provided data processing and other administrative services to Flo (and Plaintiffs  
2 maintain Flo is a “provider of healthcare”) and because the app events were transmitted for purposes  
3 of encoding them into analytics metrics and anonymizing them into aggregated dashboards.  
4

5 **Reference source as to authorization requirement and disclosures that do not require patient**  
6 **authorization. Civ. Code § 56.10(a) & (c) (2017 version)**

7 (a) A provider of health care, health care service plan, or contractor shall not disclose medical  
8 information regarding a patient of the provider of health care or an enrollee or subscriber of a health  
9 care service plan without first obtaining an authorization, except as provided in subdivision (b) or  
10 (c).

11 (c) A provider of health care or a health care service plan may disclose medical information as  
12 follows:

13 ...  
14 (3) The information may be disclosed to a person or entity that provides billing, claims  
15 management, medical data processing, or other administrative services for providers of health care  
16 or health care service plans or for any of the persons or entities specified in paragraph (2).  
17 However, information so disclosed shall not be further disclosed by the recipient in a way that  
18 would violate this part.

19 ...  
20 (16) The information may be disclosed to a third party for purposes of encoding, encrypting, or  
21 otherwise anonymizing data. However, no information so disclosed shall be further disclosed by  
22 the recipient in a way that would violate this part, including the unauthorized manipulation of  
23 coded or encrypted medical information that reveals individually identifiable medical information.  
24  
25  
26  
27  
28

STIPULATED INSTRUCTION NO. 17:

ELEMENTS OF PLAINTIFFS' CLAIM FOR VIOLATION OF THE CALIFORNIA INVASION  
OF PRIVACY ACT ("CIPA"), CAL. PENAL CODE § 632 AGAINST META

*Brought only by Plaintiffs Chen, Gamino, and Wellman*

Plaintiffs Chen, Gamino, and Wellman claim that Meta violated their right to privacy. To  
establish this claim, these Plaintiffs must prove all of the following:

1. That Meta intentionally eavesdropped on or recorded these Plaintiffs' conversations  
by using an electronic device;
2. That these Plaintiffs had a reasonable expectation that their conversations were not  
being overheard or recorded; and
3. That Meta did not have the consent of all parties to the conversations to eavesdrop  
on or record eavesdrop on them.

**Source:** CACI No. 1809.

DISPUTED INSTRUCTION NO. 18:

DEFINITION OF “EAVESDROP” UNDER CIPA § 632

**OFFERED BY PLAINTIFFS CHEN, GAMINO, AND WELLMAN**

To “eavesdrop” means to, or to attempt to, overhear or intercept others’ private communication in a clandestine or secretive manner. It is never a secret to one party to a conversation that the other party is listening to the conversation; only a third party can listen secretly to a private conversation.

1 ***Plaintiffs’ Position:***

2 There is no model instruction that provides an appropriate definition of “eavesdrop” in the  
3 context of CIPA § 632 or comparable causes of action.

4 The first sentence of Plaintiffs’ proposed instruction is derived from *Matera v. Google Inc.*,  
5 which states: “Google ignores that Black’s Law Dictionary provides a second definition of  
6 eavesdropping, which is ‘a clandestine attempt to overhear or intercept others’ private  
7 communication.’ See Black’s Law Dictionary (10th ed. 2014). The alleged interception, scanning,  
8 and analysis of Plaintiff’s private communications fall squarely within this definition of  
9 eavesdropping.” 2016 WL 8200619 (N.D. Cal. Aug. 2, 2016). The first sentence of Meta’s proposed  
10 instruction is comparable, but less clear, because it speaks only of listening to conversations, when  
11 the relevant concept of eavesdropping is broader than hearing audible conversations.  
12

13 The second sentence of Plaintiffs’ proposed instruction is derived from *Rogers v. Ulrich*, 52  
14 Cal. App. 3d 894, 898 (Ct. App. 1975), which states: “It is never a secret to one party to a  
15 conversation that the other party is listening to the conversation; only a third party can listen secretly  
16 to a private conversation.” It is identical to the second sentence of Meta’s proposed instruction.  
17

18 The third sentence of Meta’s proposed instruction is inappropriate because it misleadingly  
19 suggests a factual issue that Plaintiffs contend is not present in this case. This poses a substantial  
20 risk of confusing the jury. Meta has not established or provided any credible basis to believe it will  
21 establish a factual foundation for the notion that the Meta received the communications through a  
22 “secondhand repetition of the contents of a conversation.” Moreover, expressly including the  
23 sentence Meta is proposing poses a substantial risk of confusing the jury by implying that it describes  
24 a sharp ***additional*** aspect to the rule that requires consideration, when in reality Plaintiffs’ proposed  
25 instruction already clearly states one must eavesdrop upon the relevant private communication.  
26  
27  
28

1 DISPUTED INSTRUCTION NO. 18:

2 DEFINITION OF “EAVESDROP” UNDER CIPA § 632

3 **OFFERED BY META**

4 *Claim brought only by Plaintiffs Chen, Gamino, and Wellman*

5 To “eavesdrop” means to listen secretly to what is said in private. It is never a secret to one  
6 party to a conversation that the other party is listening to the conversation; only a third party can  
7 listen secretly to a private conversation. Any secondhand repetition of the contents of a conversation  
8 does not qualify as eavesdropping.

9 ***Sources:***

10 *No model instruction exists.*

11  
12 *Smith v. LoanMe, Inc.*, 11 Cal. 5th 183, 200 (2021) (“While one who imparts private information  
13 risks the betrayal of his confidence by the other party, a substantial distinction has been recognized  
14 between the secondhand repetition of the contents of a conversation and its simultaneous  
dissemination to an unannounced second auditor, whether that auditor be a person or mechanical  
device.”).

15 *Rogers v. Ulrich*, 52 Cal. App. 3d 894, 898 (Ct. App. 1975) (noting “‘eavesdrop’ is defined in  
16 Webster’s 7th New Collegiate Dictionary (1972) as ‘to listen secretly to what is said in private.’ It  
17 is never a secret to one party to a conversation that the other party is listening to the conversation;  
only a third party can listen secretly to a private conversation.”).

**Defendant Meta's Position:**

The jury should be instructed on how California courts have defined the term “eavesdrop” under CIPA § 632. While California courts have started with the dictionary definition of “eavesdropping” to interpret § 632, they have applied two key principles from this definition that are intuitive, but not necessarily obvious from the dictionary definition alone. *See, e.g., Rogers v. Ulrich*, 52 Cal. App. 3d 894, 899 (Ct. App. 1975) (“‘Eavesdropping’ is the problem the Legislature meant to deal with; ‘eavesdrop’ is defined in Webster’s 7th New Collegiate Dictionary (1972) as ‘to listen secretly to what is said in private.’”).

First, “only a third party can listen secretly to a private conversation” because “[i]t is never a secret to one party to a conversation that the other party is listening to the conversation.” *Rogers*, 52 Cal. App. 3d at 899; *see also People v. Drennan*, 84 Cal. App. 4th 1349, 1357 (2000) (“‘Eavesdropping’ is notably a term that refers to the surreptitious overhearing of conversations.”). The parties agree that the instruction should reflect this principle.

Second, there is a “critical distinction between eavesdropping upon or recording a conversation and later disseminating its contents.” *Flanagan v. Flanagan*, 27 Cal. 4th 766, 775, 41 P.3d 575, 581 (2002). “While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device.” *Smith v. LoanMe, Inc.*, 11 Cal. 5th 183, 200 (2021).

The jury must understand this principles to appropriately render its verdict, so Meta submits that the Court should instruct the jury as to the meaning of “eavesdropping” under California decisional law interpreting CIPA § 632.

The Court should reject Plaintiffs’ proposed instruction. It risks seriously confusing and misleading the jury in two ways. First, it suggests liability even where Meta heard *nothing*, on the theory that a mere *attempt* to listen in on a conversation is enough. Unlike other provisions of CIPA, which expressly include an “attempt to” to invade privacy, Section 632 solely covers actual eavesdropping. *Compare* Cal. Pen. Code § 631 (addressing “attempts to read” contents of



1 communication without authorization). That the Legislature did not include such language in  
2 Section 632 makes clear that it did not intend to reach “attempted eavesdropping.” Second,  
3 Plaintiffs’ proposed instruction would penalize “intercept[ing]” their communications. But  
4 California cases addressing Section 632 have drawn a distinction between “interception”—a word  
5 that doesn’t appear in Section 632—and “eavesdropping.” Section 632 does *not* reach capturing a  
6 message and then relaying its contents later. *Smith*, 11 Cal. 5th at 200. In short, Plaintiffs are trying  
7 to significantly water down their burden of proof by suggesting that the jury may find liability based  
8 on an “attempt[ed]” “interception” alone, instead of actual eavesdropping.

9 Plaintiffs also offer no serious justification for their proposed instruction. They cite only  
10 one federal district court’s decision, which turns out to contain only an analysis of whether CIPA  
11 “section 631 applies to email communications.” *Matera v. Google Inc.*, 2016 WL 8200619, \*17  
12 (N.D. Cal. Aug. 12, 2016). Section 631 is not at issue here, and that should be the end of the matter.  
13 In any event, the *Matera* court did not decide any claim asserted under Section 632 and mused  
14 about the scope of the dictionary definition of “eavesdropping” only in the course of deciding how  
15 broadly CIPA sweeps; the court decided the California Legislature intended it to reach later-  
16 developed technologies like email. *Id.* at \*19. Instead of relying on one district court’s generalized  
17 discussion about the ambit of CIPA—in a case addressing only whether to exercise supplemental  
18 jurisdiction over, and then whether to dismiss, a Section 631 claim—this Court should instead rely  
19 on the long line of California cases addressing the meaning of “eavesdropping” under Section 632.  
20  
21  
22  
23  
24  
25  
26  
27  
28

DISPUTED INSTRUCTION NO. 19:

DEFINITION OF “INTENTIONALLY” UNDER CIPA § 632

**OFFERED BY PLAINTIFFS CHEN, GAMINO, AND WELLMAN**

To act intentionally for the purposes of CIPA means to have the purpose or desire of recording a confidential conversation, or to act with the knowledge to a substantial certainty that the use of the recording equipment at issue will result in recording a confidential conversation. A party’s motive, *i.e.*, whether they had a good or evil purpose for the recording, is irrelevant. For purposes of this instruction, Plaintiffs allege that the recording equipment is Meta’s Software Development Kit (or SDK).

***Plaintiffs' Position:***

There is no model instruction that provides an appropriate definition of intentionally in the context of CIPA § 632 or comparable causes of action. The substance of this instruction is derived from *Gladstone v. Amazon Web Servs., Inc.*, which states: “[T]he recording of a confidential conversation is intentional if the person using the recording equipment does so with the purpose or desire of recording a confidential conversation, or with the knowledge to a substantial certainty that his use of the equipment will result in the recordation of a confidential conversation.” 739 F. Supp. 3d 846, 859 (W.D. Wash. 2024).

Meta’s alternative proposed instruction is inappropriate because it misleadingly describes the requisite intent requirement in terms of specific intent, as opposed to general intent. Meta’s own cited case demonstrates that this is a mistake of law, as the quote Meta provided demonstrates: “We conclude that a necessary element of the offense proscribed by former section 653j is an intent to record a confidential communication.” *People v. Superior Court of Los Angeles Cnty.*, 70 Cal. 2d 123, 133 (1969) (emphasis added to “a,” which signifies a general intent to record “a” confidential communication, rather than “the” specific communication at issue); *see also United States v. Christensen*, 828 F.3d 763, 774 (9th Cir. 2015) (intent was satisfied because the defendant “knew or had reason to know that *the design* of [the mechanical or other] device rendered it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.”); *see also Lopez v. Apple, Inc.*, 519 F. Supp. 3d 672, 684 (N.D. Cal. 2021) (“interception may be considered intentional ‘where a defendant is aware of a defect causing the interception but takes no remedial action.’”) (quoting *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 815 (N.D. Cal. 2020)); *e.g., In re Carrier IQ, Inc.*, 78 F. Supp. 3d 1051, 1059 (N.D. Cal. 2015) (wiretapping found where third-party “designed” the “software” that was then embedded into mobile device, which led software to transmit data).

1 Meta advocated for an improperly narrow view of intent—similar to the one in its proposed  
2 instruction—at summary judgment. *See* ECF No. 527 at 13-14. Notably, Plaintiffs have never, for  
3 example, proffered evidence that Meta *specifically* intended to record Plaintiff Sarah Wellman’s  
4 communications with Flo Health through the Flo App. Thus, while the Court did not explicitly  
5 address the requisite standard for intent in its summary judgment opinion, it implicitly rejected  
6 Meta’s position, by denying Meta’s motion for summary judgment. ECF No. 608 at 1-2. At trial,  
7 Plaintiffs will establish intent consistently with the accepted (general) intent requirement as  
8 articulated in *Gladstone*.  
9

10 Notably, when ruling on Google’s summary judgment motion last year, the Court also  
11 engaged with the issue of the definition of the requisite concept of intent. *See* ECF No. 485 at 7.  
12 There, the Court stated it was accepting Google’s position that the federal wiretap act and CIPA  
13 used the same operative concepts and then concluded that the “operative question” is “whether the  
14 defendant acted consciously and deliberately with the goal of intercepting wire communications.”  
15 *Id.* (citing *United States v. Christensen*, 828 F.3d 763, 775 (9th Cir. 2015)). This definition is  
16 consistent with the (general) intent definition Plaintiffs propose. In contrast, Meta’s proposal is in  
17 conflict with this definition, because it seeks to read a specific intent requirement into the definition  
18 by stating one must have intended to record “the” confidential communication.  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

DISPUTED INSTRUCTION NO. 19:

## DEFINITION OF “INTENTIONALLY” UNDER CIPA § 632

## OFFERED BY META

*Claim brought only by Plaintiffs Chen, Gamino, and Wellman*

To act intentionally means to act deliberately and purposefully. That is, the defendant’s acts must have been the product of the defendant’s conscious objective to eavesdrop on the confidential conversation in question without consent rather than the product of a mistake or accident.

***Sources:***

5 Modern Federal Jury Instructions-Civil P 92.03 (2025) (defining intentionally under Federal Wiretap Act) (as modified in redline).

*Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 126 (N.D. Cal. 2020) (“The analysis for a violation of CIPA is the same as that under the federal Wiretap Act.”).

*People v. Superior Court of Los Angeles Cnty.*, 70 Cal. 2d 123, 133 (1969) (“Fairly read, the statute does not isolate the actor’s intent from the object to which it is directed, namely the confidential communication; the two are inextricably bound together.... We reject Smith’s contention that the mere intent to activate a tape recorder which subsequently ‘by chance’ records a confidential communication is sufficient to constitute an offense under the section. We conclude that a necessary element of the offense proscribed by former section 653j is an intent to record a confidential communication.”).

***Defendant Meta's Position:***

CIPA 632 forbids “intentionally” eavesdropping on or recording confidential communications, and the Parties agree that the jury should be instructed on what “intentionally” means. Meta’s proposed instruction is modeled on the Modern Federal Jury Instruction defining “intentionally” under the Federal Wiretap Act. *See Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 126 (N.D. Cal. 2020) (“The analysis for a violation of CIPA is the same as that under the federal Wiretap Act.”); *cf.* Standing Order for Civil Jury Trials Before Judge James Donato ¶ 7 (instructing parties to “use the Ninth Circuit Model Jury Instructions to the fullest extent possible”). Meta modified that instruction slightly to account for the fact that the relevant claim here is under California Penal Code Section 632 and to reflect the foundational California Supreme Court decision on that statute, *People v. Superior Court*, 70 Cal. 2d 123 (1969) (“*Smith*”), and subsequent authorities. Plaintiffs’ proposed instruction, by contrast, boils down to an out-of-context quote from a case applying *Smith* in very different circumstances and does not provide relevant guidance on how to interpret the word “intentional” here.

Courts have made clear that the word “intentionally” requires plaintiffs to prove that the defendant acted with the conscious goal of eavesdropping or recording confidential communications, and not merely that the defendant deliberately set up a device that turned out to overhear or record such communications. For example:

- In *Smith*, the California Supreme Court, interpreting the predecessor of Section 632, held that “the statute does not isolate the actor’s intent from the subject to which it is directed.” 70 Cal. 2d at 133. In other words, “it is not the purpose of the statute to punish a person who intends to make a recording but only a person who intends to make a recording of a confidential communication.” *Id.* That means “the mere intent to activate a tape recorder” is not enough; there must be “an intent to record a confidential communication.” *Id.*
- The California Supreme Court revisited the point in *Estate of Kramme*, 20 Cal. 3d 567 (1978), in which it made clear that the law demands “an intent to record a confidential communication, rather than simply an intent to turn on a recording apparatus which happened to record a confidential communication.” *Id.* at 572 n.5.

- The California Courts of Appeal have applied that approach in other cases to conclude that Section 632 plaintiffs had either not alleged or not proven that the defendant eavesdropped on or recorded their communications intentionally. *E.g., Lozano v. City of Los Angeles*, 73 Cal. App. 5th 711, 727–28 (2022) (evidence showed the defendant “understood it was deploying recording devices that might happen to record a confidential communication—not that the [defendant] intended to record those communications”).
- Recently, Judge Chhabria, in *Doe I v. Google LLC*, 2025 WL 1616720 (N.D. Cal. June 6, 2025), applied the same approach as well, making clear that the question of intent under Section 632 “is not whether [the defendant] intended to collect any old communication,” but “whether [the defendant] intended to collect the kinds of communications at issue in this lawsuit,” *i.e.*, “private health information.” *Id.* at \*1–2.

In short, Plaintiffs must prove that Meta intended to collect their confidential health information. Meta’s proposed instruction makes that simple point. Plaintiffs take it an unjustified step further, suggesting that the Court tell the jury *both* that Meta needed to have a “purpose or desire” of listening in on a confidential communication *and* that Meta’s “motive,” whether “good or evil,” is irrelevant. This is an unnecessary complication that will serve only to confuse the jury and invite hypothetical discussions about the distinction between purposes, desires, and motives. Using the simple modified model instruction for wiretapping claims would avoid these problems.

California courts have highlighted the perils of confusing instructions on Section 632’s *mens rea* element. In *Marich v. MGM/UA Telecommunications, Inc.*, 113 Cal. App. 4th 415 (2003), for example, the Court of Appeal reversed a judgment for the defendants following a jury verdict because the trial court had given an incorrect instruction, inconsistent with the holding of *Smith*, on the meaning of the word “intentionally.” “The jury’s confusion over the court’s definition of intentional was manifest,” prompting questions from jurors and even additional closing arguments from counsel. *Id.* at 428. This Court should avoid any similar confusion here and instruct the jury that Plaintiffs must prove that Meta deliberately set out to eavesdrop on Plaintiffs’ confidential conversations with Flo.

STIPULATED INSTRUCTION NO. 19:

DEFINITION OF “CONSENT” UNDER CIPA § 632

A plaintiff may express consent by words or acts that are reasonably understood by another person as consent. A plaintiff may also express consent by silence or inaction if a reasonable person would understand that the silence or inaction intended to indicate consent.

**Sources:** CACI No. 1032 (Consent Explained).



STIPULATED INSTRUCTION NO. 20:

ELEMENTS OF PLAINTIFFS' COMMON LAW INVASION OF PRIVACY AND INTRUSION  
UPON SECLUSION CLAIM AGAINST FLO

Plaintiffs claim that Flo violated their right to privacy. To establish this claim, Plaintiffs must prove all of the following:

1. That Plaintiffs had a reasonable expectation of privacy over the custom app events transmitted by the Meta SDK;
2. That Flo intentionally intruded in into Plaintiffs' privacy by transmitting the custom app events;
3. That Flo's intrusion would be highly offensive to a reasonable person;
4. That Plaintiffs were harmed; and
5. That Flo's conduct was a substantial factor in causing Plaintiffs' harm.

In deciding whether Plaintiffs had a reasonable expectation of privacy over the custom app events at issue, you should consider, among other factors, the following:

- (a) The identity of Flo;
- (b) The extent to which other persons had access to similar information about Plaintiffs and could see or hear Plaintiffs; and
- (c) The means by which the intrusion occurred.

In deciding whether an intrusion is highly offensive to a reasonable person, you should consider, among other factors, the following:

- (a) The extent of the intrusion;
- (b) Flo's motives and goals; and
- (c) The setting in which the intrusion occurred.

**Source:** CACI No. 1800.

DISPUTED INSTRUCTION NO. 21:

RE “HIGHLY OFFENSIVE”

**OFFERED BY FLO**

“Highly offensive” means that the disclosure constitutes an egregious breach of social norms. Disclosure of device identifier numbers, personal data, and geolocation from a user’s device is not considered to be an egregious breach of social norms.

***Defendant Flo's Position:***

Though CACI 1800 sets forth the elements of a common law invasion of privacy claim, it is not tailored to the allegations that are specific to this case, *i.e.* whether, in connection with the use of the Flo Health mobile application, Flo violated Plaintiffs' privacy. Case law from within this district provides additional context for the jury to consider in evaluating Plaintiffs' invasion of privacy claim. Citing precedent from the California Supreme Court, this court clarified that "[a]ctionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right." *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (citing *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 37 (1994)). The Court thereafter applied that standard as follows:

Here, the information allegedly disclosed to third parties included the unique device identifier number, personal data, and geolocation information from Plaintiffs' iDevices. Even assuming this information was transmitted without Plaintiffs' knowledge and consent, a fact disputed by Defendants, such disclosure does not constitute an egregious breach of social norms.

*Id.* (citing *Fogelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011) ("Here, the supposed invasion of privacy essentially consisted of [Defendant] obtaining plaintiff's address without his knowledge or permission, and using it to mail him coupons and other advertisements. This conduct is not an egregious breach of social norms, but routine commercial behavior."))

Because of the technology at issue, Flo respectfully submits that an instruction on what does or does not constitute a "highly offensive" act in this setting—separate and apart from the general definition set forth in CACI 1800—will be useful to the jury.

1 ***Plaintiffs' Position:***

2 Flo's proposed instruction should be deleted. The parties agreed to use CACI No. 1800 as  
3 the model language for the instruction of common law intrusion upon seclusion. That model  
4 instruction already **explicitly** defines "highly offensive." It would be confusing to the jury to provide  
5 a separate competing definition of the same term for purposes of defining the same element of that  
6 claim.  
7

8 Moreover, Flo's instruction is not based on any model and is deeply inappropriate. It does  
9 not merely seek to define a term but asserts a factual conclusion that disclosing "personal data" is  
10 never "highly offensive." That makes no sense and does not follow from the case Flo cites. Rather,  
11 Flo's cited case addresses "negligent conduct that leads to theft of highly personal information"—it  
12 is bound by its circumstances—and it did not hold that sharing personal data could never be highly  
13 offensive, but merely found the conduct at issue fell short of being highly offensive. *In re iPhone*  
14 *Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012). Additionally, the data at issue in  
15 the *iPhone* case was not the sort of sensitive health information at issue here. Finally, another  
16 District Court's decision on a motion to dismiss is not controlling as to the jury's right to determine  
17 what conduct is highly offensive and the existence of an out-of-context quote from another case  
18 should not provide a basis to overrule a directly on point instruction in CACI.  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

STIPULATED INSTRUCTION NO. 22:

RE “SUBSTANTIAL FACTOR”

A substantial factor in causing harm is a factor that a reasonable person would consider to have contributed to the harm. It must be more than a remote or trivial factor. It does not have to be the only cause of the harm.

Conduct is not a substantial factor in causing harm if the same harm would have occurred without that conduct.

***Source:*** CACI No. 430

STIPULATED INSTRUCTION NO. 23:

ELEMENTS OF PLAINTIFFS' INVASION OF PRIVACY AND VIOLATION OF THE  
CALIFORNIA CONSTITUTION ART. 1 § 1 CLAIM AGAINST FLO

Plaintiffs, as Class Representatives, bring an invasion of privacy claim against Flo under the California Constitution. To establish this claim, Plaintiffs, as Class Representatives, must prove by a preponderance of the evidence:

1. Plaintiffs possess a legally protected privacy interest;
2. Plaintiffs maintain a reasonable expectation of privacy; and
3. The intrusion is so serious as to constitute an egregious breach of the social norms such that the breach is "highly offensive."

**Source:** *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1075 (N.D. Cal. 2021).

DISPUTED INSTRUCTION NO. 24:

OBJECTIVELY REASONABLE EXPECTATION OF PRIVACY

**OFFERED BY FLO**

In deciding whether Plaintiffs had a reasonable expectation of privacy over the custom app events transmitted on the Flo app, you should consider, among other factors, the following:

- (a) The identity of Flo;
- (b) The extent to which other persons had access to the custom app events transmitted and could see or hear Plaintiffs;
- (c) The means by which the intrusion occurred.

**Source:** CACI No. 1800.

***Defendant Flo's Position:***

No CACI exists for constitutional invasion of privacy claims because Cal. Const. Art. 1, § 1 “identifies mere principles and does not create a private right of action.” *Crossley v. California*, 479 F. Supp. 3d 901, 918 (S.D. Cal. 2020) (emphasis added) (collecting cases). However, to the extent courts have permitted such claims, they have incorporated the same “highly offensive” and “reasonable expectation of privacy” standards as for common law claims. Accordingly, CACI No. 1800, which defines those elements in the common law context, should be given to clarify these same terms in the constitutional claims context.



1 ***Plaintiffs' Position:***

2 Flo's proposed instruction should be deleted. The parties agreed to use CACI No. 1800 as  
3 the model language for the instruction of common law intrusion upon seclusion. That model  
4 instruction already **explicitly** defines "objectively reasonable expectation of privacy." There is no  
5 legal reason to provide a different instruction of "objectively reasonable expectation of privacy" in  
6 the context of Plaintiffs' invasion of privacy claim under the California Constitution.  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

DISPUTED INSTRUCTION NO. 25:

RE HIGHLY OFFENSIVE

**OFFERED BY FLO**

“Highly offensive” means that the disclosure constitutes an egregious breach of social norms. Disclosure of device identifier numbers, personal data, and geolocation from a user’s device is not considered to be an egregious breach of social norms.

***Source:*** *In re iPhone Application Litigation*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012)

***Defendant Flo's Position:***

Flo's definition of highly offensive will be helpful to the jury in assessing the issues in this case, *i.e.*, whether, in connection with the use of the Flo mobile application, Flo violated Plaintiffs' privacy. Additional case law from within this district provides additional context for the jury to consider in evaluating Plaintiffs' invasion of privacy claim. Citing precedent from the California Supreme Court, prior courts in this district clarified that "[a]ctionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right." *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (citing *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 37 (1994)). The Court thereafter applied that standard as follows:

Here, the information allegedly disclosed to third parties included the unique device identifier number, personal data, and geolocation information from Plaintiffs' iDevices. Even assuming this information was transmitted without Plaintiffs' knowledge and consent, a fact disputed by Defendants, such disclosure does not constitute an egregious breach of social norms.

*Id.* (citing *Fogelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011) ("Here, the supposed invasion of privacy essentially consisted of [Defendant] obtaining plaintiff's address without his knowledge or permission, and using it to mail him coupons and other advertisements. This conduct is not an egregious breach of social norms, but routine commercial behavior.")).

Because of the technology at issue, Flo respectfully submits that an instruction on what does or does not constitute a "highly offensive" act in this setting—separate and apart from the general definition set forth in CACI 1800—will be useful to the jury.

1 ***Plaintiffs’ Position:***

2 Flo’s proposed instruction should be deleted. The parties agreed to use CACI No. 1800 as  
3 the model language for the instruction of common law intrusion upon seclusion. That model  
4 instruction already **explicitly** defines “highly offensive.” There is no legal reason to provide a  
5 different instruction of highly offensive in the context of Plaintiffs’ invasion of privacy claim under  
6 the California Constitution.  
7

8 Moreover, Flo’s instruction is not based on any model and is deeply inappropriate. It does  
9 not merely seek to define a term but asserts a factual conclusion that disclosing “personal data” is  
10 never “highly offensive.” That makes no sense and does not follow from the case Flo cites. Rather,  
11 Flo’s cited case addresses “negligent conduct that leads to theft of highly personal information”—it  
12 is bound by its circumstances—and it did not hold that sharing personal data could never be highly  
13 offensive, but merely found the conduct at issue fell short of being highly offensive. *In re iPhone*  
14 *Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012). Additionally, the data at issue in  
15 the *iPhone* case was not the sort of sensitive health information at issue here. Finally, another  
16 District Court’s decision on a motion to dismiss is not controlling as to the jury’s right to determine  
17 what conduct is highly offensive and the existence of an out-of-context quote from another case  
18 should not provide a basis to overrule a directly on point instruction in CACI.  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

STIPULATED INSTRUCTION NO. 26:

SUBSTANTIAL FACTOR

A substantial factor in causing harm is a factor that a reasonable person would consider to have contributed to the harm. It must be more than a remote or trivial factor. It does not have to be the only cause of the harm.

Conduct is not a substantial factor in causing harm if the same harm would have occurred without that conduct.

***Source:*** CACI No. 430

STIPULATED INSTRUCTION NO. 27:

## ELEMENTS OF PLAINTIFFS' BREACH OF CONTRACT CLAIM AGAINST FLO

Plaintiffs claim that they and Flo entered into a contract as set forth in the Flo App Terms of Service and Privacy Policy, which state the types of information Flo represented it would and would not disclose.

Plaintiffs claim that Flo breached this contract by transmitting the 12 custom app events at issue to Meta and Google.

Plaintiffs also claim that Flo's breach of this contract caused harm to Plaintiffs for which Flo should pay.

Flo denies that it breached the contracts because the Terms of Service and Privacy Policy specifically disclosed the data sharing practices Plaintiffs challenge. Flo also claims Plaintiffs' claims are barred by the statute of limitations.

**Source:** CACI No. 300

To recover damages from Flo for breach of contract, Plaintiffs must prove all of the following:

1. That Plaintiffs and Flo entered into a contract;
2. That Plaintiffs did all, or substantially all, of the significant things that the contract required them to do;
3. That Flo did something that the contract prohibited it from doing;
4. That Plaintiffs were harmed; and
5. That Flo's breach of contract was a substantial factor in causing Plaintiffs' harm.

**Source:** CACI No. 303

DISPUTED INSTRUCTION NO. 28:

THE CONTRACT

**OFFERED BY FLO**

Plaintiffs and Flo agreed to be bound by all versions of Flo's Terms of Service and Privacy Policy applicable during the Class Period. Plaintiffs and Flo agree that contract consists of the applicable versions of Flo's Terms of Service and Privacy Policy in place during the Class Period.

1     ***Defendant Flo's Position***

2             In order for Plaintiffs to have a viable breach of contract claim under California, Plaintiffs  
3     must acknowledge that they entered into a contract. A fundamental tenant of entering into a contract  
4     is that the parties *agreed* to the terms of the contract. *See* CACI 302, Contract Formation—Essential  
5     Factual Elements (“To prove that a contract was created, [Plaintiffs] must prove all of the following:  
6     (1) That the contract terms were clear enough that the parties could understand what each was  
7     required to do; (2) That the parties agreed to give each other something of value[]; and (3) That the  
8     parties *agreed* to the terms of the contract.”) (emphasis added). Thus, Flo respectfully submits that  
9     the jury must be instructed not only that there was a contract, but that Plaintiffs agreed to the terms  
10    of those contracts. No contract, let alone a viable claim for a breach of contract, can exist without  
11    an agreement to be bound by the contract’s terms.



1 ***Plaintiffs' Position:***

2 Plaintiffs do not believe this instruction should be given. It is not based off of any model  
3 instruction. Defendants already filed a motion in limine (ECF No. 645 (Defs' MIL 2) that sought to  
4 resolve fact issues concerning the applicability of contract terms prior to trial, and this motion was  
5 rejected by the Court. ECF No. 692. Flo's attempt to impose a factual conclusion concerning the  
6 effect of certain privacy policies through a jury instruction is improper for the same reasons that  
7 motion in limine was improper. This instruction merely seeks to instruct the jury on how (*i.e.*, which  
8 way) to resolve fact issues, and is therefore entirely improper. That Plaintiffs allege a breach of  
9 contract claim does not, as Flo claims, mean Plaintiffs "agreed to be bound by all versions of Flo's  
10 Terms of Service and Privacy Policy." For example, Flo modified its privacy policy mere days  
11 before the end of the Class Period, and the applicability of that privacy policy would be subject to  
12 substantial fact dispute.

DISPUTED INSTRUCTION NO. 29:

## INTERPRETATION OF THE CONTRACT

**OFFERED BY FLO**

Plaintiffs and Flo dispute the meaning of the following words in their contract:

- To provide and support the services we provide to you, information we collect and receive may be disclosed to third parties.
- We may share information, including personally identifying information, with our affiliates (companies that are part of our corporate groups of companies, including but not limited to Facebook) to help provide, understand and improve our application.
- We may also generally disclose aggregate or anonymous information when reasonable steps have been taken to ensure the data does not contain your personally identifying information.
- Other ways we use your data include developing aggregated analyses and reports that help us improve our application, understand how our application is used and to improve our products. We also use your information to communicate with you, such as sending you notifications and service-related messages, or by responding to your requests and questions.
- When you access or use the App, we may automatically collect the following information:
  - Device Information: We collect information about the mobile device you use to access the App, including the hardware model, operating system and version, unique device identifiers and mobile network information.
  - Location Information: We collect your IP address, time zone, and information about your mobile service provider, which allows us to infer your general location.
  - Information Collected by Cookies and Other Tracking Technologies: We use various technologies to collect information about your use of the App, such as frequency of use, which areas and features of our App you visit and your use patterns generally, engagement tracking with particular features, etc. To collect this information, we may send cookies to your mobile device or computer. Cookies are small data files stored on your hard drive or in device memory.
- We may use your information, including your Personal Data, for the following purposes:
  - 1. to analyze, operate, maintain and improve the App, to add new features and services to the App;
  - 2. to customize content you see when you use the App;
  - 3. to provide and deliver the products and services you request, process transactions and send you related information, including confirmations and reminders;
  - 4. to customize product and service offerings and recommendations to you, including third-party products and offerings (except data from Apple HealthKit and Google Fit);

- 9. to monitor and analyze trends, usage and activities in connection with our App;
- 13 for any other purposes disclosed to you at the time we collect Personal Data or any other purposes indicated in this Privacy Policy.

- Among others we may share your Personal Data with the following third-party services: .... Facebook and Google. We use Facebook Analytics and Google Analytics tools to track installs of our App. Normally, Facebook and Google collect only non-personally identifiable information, though some Personal Data like device identifiers may be transferred to Facebook and Google. Read more about analytical services provided by Facebook here . And by Google here. . You can find their data practices in ‘Privacy’ sections.
- BY USING THE APP, YOU CONSENT THAT WE MAY USE COOKIES AND THIRD-PARTY SERVICES, AND COLLECT YOUR USAGE DATA UNDER A UNIQUE IDENTIFIER, FOR THE PURPOSES OF TRACKING, ANALYSIS, AND IMPROVEMENT OF THE APP.
- If the information covered by this Section is aggregated or de-identified so it is no longer reasonably associated with an identified or identifiable natural person, we may use it for any business purpose.

Plaintiffs claim that the words mean [insert plaintiff’s interpretation]. Flo claims that the words mean: (1) Flo was permitted to use custom app events and Meta and Google’s SDKs to perform analytics to monitor and improve the app; (2) Flo was permitted to transmit the information at issue in this case through the Meta and Google SDKs; (3) Flo was permitted to share user data with third-party analytics companies, including Meta and Google; and (4) Flo was permitted to share device identifiers through the Meta and Google SDKs; (5) Flo was permitted to use user data for targeted content within the App; and (6) Flo could use de-identified or aggregated data for any purpose. Plaintiffs must prove that their interpretation is correct.

In deciding what the words of a contract mean, you must decide what the parties intended at the time the contract was created. You may consider the usual and ordinary meaning of the language used in the contract as well as the circumstances surrounding the making of the contract.

The following instructions may also help you interpret the words of the contract:

1 ***Defendant Flo's Position:***

2 CACI 314 is unnecessary in this case. As the directions make clear, this instruction should  
3 only be given "if there is conflicting extrinsic evidence as to what the parties intended the language  
4 of their contract to mean." Here, extrinsic evidence is not necessary to interpret the contract. Indeed,  
5 Plaintiffs have put forth no extrinsic evidence at all supporting their interpretation of the Flo Terms  
6 of Use and Privacy Policy.  
7

8 However, if this instruction is to be given, it should be given as set forth in the CACI,  
9 including copying the CACI text verbatim and setting forth the disputed language verbatim and  
10 competing interpretations in detail. As noted below, the instruction regarding Plaintiffs' proposed  
11 *contra proferentem* instruction modeled on CACI No. 320 should not be given without CACI 314.  
12 The two go hand-in-hand, as is made clear by the Judicial Council's directions for CACI No. 314.  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

DISPUTED INSTRUCTION NO. 29:

INTERPRETATION OF THE CONTRACT

**OFFERED BY PLAINTIFFS**

In determining the meaning of the words of the contract, if you have considered all of the instructions I've given you, circumstances, and evidence before you, and yet still cannot agree on the meaning of the words, then you should interpret the contract against the party that drafted the disputed words and thus is the party that caused the uncertainty.

1 ***Plaintiffs' Position:***

2 This instruction is modeled directly off CACI No. 320 with the addition only of "if you have  
3 considered all of the instructions I've given you, circumstances, and evidence before you, and yet"  
4 (replacing "you must first consider all of the other instructions that I have given you").

5 Plaintiffs are bewildered by Flo's disputed proposal on this instruction. Flo stated in its  
6 position statement that it believes an instruction based on CACI No. 314 is "unnecessary," and then  
7 ***added*** an instruction based on CACI No. 314 that was not included in Plaintiffs' proposal. Flo has  
8 declined offers to meet and confer and so its intent with this paradoxical position remains entirely  
9 unclear. Plaintiffs ***agree*** with Flo that CACI No. 314 is unnecessary in this case. Flo's proposed  
10 instruction should be deleted for this reason. Additionally, the text of Flo's proposal is inappropriate  
11 because it assumes which text will be in dispute, selects many provisions that will not likely be in  
12 dispute, excludes critical text that is more likely to be central to disputes—*e.g.*, the statement in  
13 Flo's privacy policy that "WE WILL NOT TRANSMIT ANY OF YOUR PERSONAL DATA TO  
14 THIRD PARTIES, EXCEPT IF IT IS REQUIRED TO PROVIDE THE SERVICE TO YOU (E.G.  
15 TECHNICAL SERVICE PROVIDERS', UNLESS WE HAVE ASKED FOR YOUR EXPLICIT  
16 CONSENT." Plaintiffs' proposal does not include an instruction based on CACI No. 314 at this  
17 time, but Plaintiffs reserve the right to suggest one may be appropriate as trial unfolds depending on  
18 the arguments raised by the parties.  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1 ***Defendant Flo's Position:***

2 CACI 320 is unnecessary in this case. As the directions to CACI No. 314 make clear,  
3 instruction 320 should only be given "if there is conflicting extrinsic evidence as to what the parties  
4 intended the language of their contract to mean." Here, Plaintiffs agree that extrinsic evidence is not  
5 necessary to interpret the contract and that CACI No. 314 need not be given. Therefore, instruction  
6 No, 320 should not be given.  
7

8 CACI 320 is also unnecessary because the *contra proferentem* principle reflected in this  
9 instruction is a principle of last resort that applies only "only as a tie breaker, when other canons fail  
10 to dispel uncertainty." *Pacific Gas & Electric Co. v. Superior Court* (1993) 15 Cal. App. 4th 576,  
11 596. Here, Plaintiffs have not identified ambiguities in what the contract means that would warrant  
12 giving this instruction. Furthermore, if this instruction is to be given, it should be given as written  
13 in the CACI, that is, along with instruction No. 314. In other words, it does make sense (and violates  
14 the CACI directions) to give only instruction No. 320 but not 314.  
15

16 Finally, if a *contra proferentem* instruction is included, the instruction should clarify that the  
17 doctrine can only be used to decide between competing "reasonable and practical constructions of  
18 an ambiguous contractual provision." *Newport Assocs. Dev. Co. v. Travelers Indem. Co. of Illinois*,  
19 162 F.3d 789 (3d Cir. 1998) (quoting *United States v. Seckinger*, 397 U.S. 203, 216 (1970)).  
20  
21  
22  
23  
24  
25  
26  
27  
28

STIPULATED INSTRUCTION NO. 30:

CONSTRUCTION OF CONTRACT AS A WHOLE

The following instructions may also help you interpret the words of the contract:

You should assume that the parties intended the words in their contract to have their usual and ordinary meaning unless you decide that the parties intended the words to have a special meaning

In deciding what the words of a contract meant to the parties, you should consider the whole contract, not just isolated parts. You should use each part to help you interpret the others, so that all the parts make sense when taken together.

In deciding what the words in a contract meant to the parties, you may consider how the parties acted after the contract was created but before any disagreement between the parties arose.

***Source:*** CACI Nos. 314, 315, 317, 318.



DISPUTED INSTRUCTION NO. 31:

CONSENT

**OFFERED BY FLO**

Flo is not responsible for Plaintiffs' harm, if any, if Flo proves that Plaintiffs consented, by words or conduct, to Flo's communication of the custom app events to others. In deciding whether Plaintiffs consented to the communication, you should consider the circumstances surrounding the words or conduct.

***Source:*** CACI 1721.

1 ***Defendant Flo's Position:***

2  
3 It is a bedrock principle of California law that that "[sh]e who consents to an act is not  
4 wronged by it." Cal. Civ. Code § 3515. This instruction regarding the affirmative defense is taking  
5 verbatim from CACI No. CACI 1721.

6 Plaintiffs' argument that this instruction should not be given as to the CMIA claim conflates  
7 Flo's *affirmative* defense of consent with the unauthorized disclosure elements Plaintiffs need to  
8 prove as part of their CMIA claim. Even assuming that Plaintiffs' correctly state the authorization  
9 that would be relevant under the CMIA, that does not go to Flo's affirmative defense of consent,  
10 which is a defense to all claims. Plaintiffs cite no authority for the proposition that the affirmative  
11 defense of consent applies only to common law claims.  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

DISPUTED INSTRUCTION NO. 31:

AFFIRMATIVE DEFENSE - CONSENT AS TO INTRUSION UPON SECLUSION, INVASION  
OF PRIVACY UNDER THE CALIFORNIA CONSTITUTION, AND BREACH OF  
CONTRACT

**OFFERED BY PLAINTIFFS**

Flo is not responsible for the harms Plaintiffs' claim for intrusion upon seclusion, invasion of privacy under the California Constitution, and breach of contract, if any, if Flo proves that Plaintiffs consented, by words or conduct, to Flo's communication of the custom app events to others. In deciding whether Plaintiffs consented to the communication, you should consider the circumstances surrounding the words or conduct. This affirmative defense does not apply to Plaintiffs' claims against Flo Health for violation of the CMIA.

1 ***Plaintiffs’ Position:***

2 Plaintiffs do not dispute the language used to describe the affirmative defense of consent as  
3 to claims to which this defense can be applied. That language is properly based on CACI 1721.

4  
5 However, **it is critically important and among the most important of the disputed jury**  
6 **instructions** that the jurors be instructed that they should **not** consider this affirmative defense in  
7 connection with Plaintiffs’ CMIA claims. The common law notion of “consent” is not an affirmative  
8 defense to a CMIA claim and, instead, such claims are subject to a statutory regime expressly  
9 defining the concept of “authorization.” While Plaintiffs’ believe any affirmative defense of consent  
10 to the CMIA is unsupported, if one were to be offered it should reflect the statutory definition of  
11 authorization.

12  
13 Flo’s proposed instruction, if applied to the CMIA, contradicts the plain language of the  
14 CMIA and improperly attempts to bypass the authorization requirements of CMIA § 56.11. The  
15 statute clearly states that a provider of health care “shall not disclose medical information regarding  
16 a patient of the provider of health care . . . without first obtaining an ***authorization.***” CMIA §  
17 56.10(a) (emphasis added). That requirement of “an authorization,” means an authorization that  
18 meets the statutory requirements in CMIA § 56.11—not any purported consent Flo wishes to  
19 manufacture from its privacy policies. To permit a general common law consent affirmative defense  
20 to apply to the CMIA would directly contravene the statutory text and clear legislative intent. While  
21 common law affirmative defenses can sometimes apply to a statutory claim, they do not, and should  
22 ever be permitted to, overrule the legislative intent behind the statute itself. Doing so would elevate  
23 general common law concepts above the express statutory provisions passed by the Legislature.  
24 Here, Flo has cited no support for the existence of a general common law affirmative defense of  
25 “consent” to a CMIA claim.  
26  
27  
28

1 Section 56.11 defines what constitutes a valid authorization for the release of medical  
2 information. It requires specific elements designed to ensure people making such authorization  
3 understand and genuinely consent to the disclosure of their sensitive health data, including:

- 4 • Clear presentation in handwritten form or at least 14-point font,
- 5 • Separation from other language with a standalone signature,
- 6 • Explicit identification of entities authorized to receive the information,
- 7 • Specific uses and limitations on the information's use,
- 8 • An expiration date, and
- 9 • Notice of the right to receive a copy.

10 These requirements are not mere technicalities—they are substantive protections ensuring  
11 that people are genuinely informed before their health information is shared and that such disclosure  
12 is robust and specific. The Legislature crafted these detailed requirements precisely because medical  
13 information deserves heightened protection.

14 Flo has offered several justifications to Plaintiffs in the past as to why it thinks it may be  
15 exempt from the authorization requirements. These arguments are meritless, but also **completely**  
16 irrelevant to whether an affirmative defense of consent is appropriate. Simply put, if Flo's data  
17 sharing was "authorized" then Flo did not violate the CMIA, if its data sharing was not authorized,  
18 then a separate common law affirmative defense of "consent" should not provide it license to ignore  
19 the statutory requirements expressly set forth in the CMIA.

DISPUTED INSTRUCTION NO. 32:

AFFIRMATIVE DEFENSE - RETROACTIVE CONSENT AS TO ALL CLAIMS

**OFFERED BY FLO**

In determining whether Plaintiffs consented, you do not need to find that Plaintiffs consented prior to using the Flo app. If at any time during the Class Period Plaintiffs consented to Flo engaging in the actions that Plaintiffs claim violated their privacy, you must find for Flo.

***Defendant Flo’s Position:***

Plaintiffs do not and cannot dispute that they agreed to be bound by the applicable privacy policies and terms of service during the Class Period. If Plaintiffs consented to the actions that form the basis of their complaint—including, by agreeing to the Terms of Service and Privacy Policy—then Plaintiffs claims are barred as a matter of law. Accordingly, because consent is an affirmative defense and there is no relevant pattern instruction in the Ninth Circuit Model Instructions, Flo submits that it is important to instruct the jury on this dispositive affirmative defense at trial.

***Source:*** *Javier v. Assurance IQ, LLC*, 2021 WL 940319, at \*3 (N.D. Cal. Mar. 9, 2021) (“[R]etroactive consent to data collection [is] valid . . . where there is no time limitation or restriction on the claims,” such as statements that “we collect” instead of “we will collect[.]”) (citations omitted); *Salgado v. Carrows Rest., Inc.*, 33 Cal. App. 5th 356, 361 (2019) (noting that agreement to arbitrate, for example, may be “applied retroactively to transactions which occurred prior to the execution of the arbitration agreement”) (citations omitted).

1 ***Plaintiffs' Position:***

2 Flo's proposed "retroactive consent" instruction is inappropriate and should be deleted  
3 because "no case shows that California has adopted retroactive consent as a defense to an invasion  
4 of privacy tort." *Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 WL 1744107 (9th Cir. May 31,  
5 2022) (Bumatay, J., concurring). The notion of implied consent described in this jury instruction  
6 has no application here, especially because, here, an actionable statutory tort-like claim accrued  
7 concurrently with Plaintiffs' first use of the Flo application, and this could not be consented to at a  
8 later time than Plaintiffs' first use of the Flo application.

9 Additionally, if an instruction for retroactive consent were given — and it should not be —  
10 any such instruction should be expressly limited to not include Plaintiffs CMIA claims. As more  
11 fully stated in Plaintiffs' position on Flo's general consent affirmative defense instruction, the CMIA  
12 includes an express statutory regime for "authorized" disclosure, with extensive text defining that  
13 concept, such that a general "consent" instruction would nullify the express statutory text.  
14 Moreover, Flo has identified no case law or other authority justifying general consent as a viable  
15 affirmative defense to a claim under the CMIA.



STIPULATED INSTRUCTION NO. 33:

STATUTE OF LIMITATIONS ON CLAIMS AGAINST FLO

Flo contends that Plaintiffs' lawsuit was not filed within the time set by law. To succeed on this defense, Flo must prove that Plaintiffs' claimed harm occurred before January 29, 2020.

**Source:** CACI No. 454.

STIPULATED INSTRUCTION NO. 34:

RE DELAYED DISCOVERY OF CLAIMS AGAINST FLO

If Flo proves that Plaintiffs' claimed harm occurred before January 29, 2020, Plaintiffs' lawsuit was still filed on time if Plaintiffs prove that before that date, Plaintiffs did not discover, and a reasonable and diligent investigation would not have disclosed, that Flo's transmission of data to Meta contributed to Plaintiffs' harm.

***Source:*** CACI No. 455 (Statute of Limitations).

STIPULATED INSTRUCTION NO. 35

AFFIRMATIVE DEFENSE TO CIPA § 632 CLAIM AGAINST META—STATUTE OF  
LIMITATIONS

Meta contends that Plaintiffs Chen, Gamino, and Wellman’s lawsuit was not filed within the time set by law. To succeed on this defense, Meta must prove each Plaintiff’s claimed harm occurred before June 7, 2020.

***Source:*** CACI No. 454.



STIPULATED INSTRUCTION NO. 37:

DAMAGES ON MULTIPLE LEGAL THEORIES

Plaintiffs seek damages from Flo under more than one legal theory. However, each item of damages may be awarded only once, regardless of the number of legal theories alleged.

You will be asked to decide whether Flo is liable to Plaintiffs under the following legal theories:

1. Common Law Invasion of Privacy – Intrusion Upon Seclusion
2. Invasion of Privacy and Violation of the California Constitution Art. 1 § 1
3. Breach of Contract

The following items of damages are recoverable only once under all of the above legal theories:

1. Nominal damages.

The following additional item of damages is recoverable only once for Plaintiffs' claims under the California Confidentiality of Medical Information Act ("CMIA"):

1. Statutory damages.

**Source:** CACI No. 3934.

DISPUTED INSTRUCTION NO. 38:

CMIA DAMAGES

**OFFERED BY FLO**

If you determine that Flo violated the CMIA, you should award each affected member of the alleged Class damages of one thousand dollars (\$1,000).

1 ***Defendant Flo’s Position:***

2 Flo submits that this is an accurate reflection of the damages to be awarded, if any, under the  
3 CMIA. Cal. Civ. Code § 56.36 provides: “In addition to any other remedies available at law, an  
4 individual may bring an action against a person or entity who has negligently released confidential  
5 information or records concerning him or her in violation of this part, for either or both of the  
6 following: (1) ... nominal damages of one thousand dollars (\$1,000).” The plain language of the  
7 statute is that each affected person can recover damages from the “person or entity” that violated the  
8 CMIA only once. The statute does not provide for damages on a “per violation” basis, and California  
9 law forbids reading such language into the statute where the legislature did not draft it.

10  
11 ***Source:*** Cal. Civ. Code § 56.36 (“In addition to any other remedies available at law, an individual  
12 may bring an action against a person or entity who has negligently released confidential information  
13 or records concerning him or her in violation of this part, for either or both of the following: (1) ...  
14 nominal damages of one thousand dollars (\$1,000).”).  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1 ***Plaintiffs' Position:***

2 An instruction as to CMIA damages is superfluous and potentially confusing for a jury  
3 because, if liability is found, the jury will not be able to decide the amount of damages, since they  
4 are set by statute.  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28



STIPULATED INSTRUCTION NO. 39:

NOMINAL DAMAGES

This instruction applies only to Plaintiffs' and Class Members' Claims against Flo for Common Law Invasion of Privacy – Intrusion Upon Seclusion, Invasion of Privacy under the California Constitution, and Breach of Contract.

The law that applies to this case authorizes an award of nominal damages. If you find for the Plaintiffs but you find that the Plaintiffs have failed to prove damages as defined in these instructions, you must award nominal damages. Nominal damages may not exceed one dollar.

**Source:** Ninth Circuit Model Civil Jury Instructions 5.6.

STIPULATED INSTRUCTION NO. 40

DUTY TO DELIBERATE

When you begin your deliberations, elect one member of the jury as your presiding juror who will preside over the deliberations and speak for you here in court.

You will then discuss the case with your fellow jurors to reach agreement if you can do so. Your verdict, whether liable or not liable, must be unanimous.

Each of you must decide the case for yourself, but you should do so only after you have considered all the evidence, discussed it fully with the other jurors, and listened to the views of your fellow jurors.

Do not be afraid to change your opinion if the discussion persuades you that you should. But do not come to a decision simply because other jurors think it is right.

It is important that you attempt to reach a unanimous verdict but, of course, only if each of you can do so after having made your own conscientious decision. Do not change an honest belief about the weight and effect of the evidence simply to reach a verdict.

Perform these duties fairly and impartially. Do not allow personal likes or dislikes, sympathy, prejudice, fear, or public opinion to influence you. You should also not be influenced by any person's race, color, religion, national ancestry, gender, sexual orientation, profession, occupation, economic circumstances, or position in life or in the community.

It is your duty as jurors to consult with one another and to deliberate with one another with a view towards reaching an agreement if you can do so. During your deliberations, you should not hesitate to reexamine your own views and change your opinion if you become persuaded that it is wrong.

**Source:** Google Play Final Instruction No. 41.

CONSIDERATION OF THE EVIDENCE -- CONDUCT OF THE JURY

Do not communicate with anyone in any way and do not let anyone else communicate with you in any way about the merits of the case or anything to do with it. This includes discussing the case in person, in writing, by phone or electronic means, via email, text messaging, or any Internet social media site, blog, website or other feature. This applies to communicating with your family members, your employer, the media or press, and the people involved in the trial. If you are asked or approached in any way about your jury service or anything about this case, you must respond that you have been ordered not to discuss the matter and report the contact to the Court.

Do not read, watch, or listen to any news or media accounts or commentary about the case or anything to do with it; do not do any research, such as consulting dictionaries, searching the Internet, or using other reference materials; and do not make any investigation or in any other way try to learn about the case on your own.

The law requires these restrictions to ensure the parties have a fair trial based on the same evidence that each party has had an opportunity to address. A juror who violates these restrictions jeopardizes the fairness of these proceedings, and a mistrial could result that would require the entire trial process to start over. If any juror is exposed to any outside information, please notify the Court immediately.

**Source:** Google Play Final Instruction No. 42.

STIPULATED INSTRUCTION NO. 42

USE OF NOTES

Some of you have taken notes during the trial. Whether or not you took notes, you should rely on your own memory of what was said. Notes are only to assist your memory. You should not be overly influenced by your notes or those of your fellow jurors.

**Source:** Google Play Final Instruction No. 43.

## COMMUNICATION WITH THE COURT

If it becomes necessary during your deliberations to communicate with me, you may send a note through Ms. Clark, signed by any one or more of you. No member of the jury should ever attempt to communicate with me except by a signed writing, and I will respond to the jury concerning the case only in writing or here in open court. If you send out a question, I will consult with the lawyers before answering it, which may take some time. You may continue your deliberations while waiting for the answer to any question. Remember that you are not to tell anyone -- including me or Ms. Clark -- how the jury stands, numerically or otherwise, on any question submitted to you, including the question of whether either of the Defendants is liable, until after you have reached a unanimous verdict or have been discharged.

**Source:** Google Play Final Instruction No. 42.

STIPULATED INSTRUCTION NO. 44

RETURN OF VERDICT

A verdict form has been prepared for you. After you have reached unanimous agreement on a verdict, your presiding juror should complete the verdict form according to your deliberations, sign and date it, and advise Ms. Clark that you are ready to return to the courtroom.

**Source:** Google Play Final Instruction No. 45.

/s/Brenda Sharton

**DECHERT LLP**

Brenda R. Sharton (pro hac vice)  
One International Place  
100 Oliver Street  
Boston, MA 02110  
Tel: (617) 728-7100  
Fax: (617) 426-6567  
brenda.sharton@dechert.com

Benjamin Sadun (SBN 287533)  
US Bank Tower  
633 West 5th Street, Suite 4900  
Los Angeles, CA 90071  
Tel: (213) 808-5700  
Fax: (213) 808-5760  
benjamin.sadun@dechert.com

*Counsel for Defendant Flo Health, Inc.*

/s/Andrew B. Clubok

**LATHAM & WATKINS LLP**

Andrew B. Clubok (pro hac vice)  
andrew.clubok@lw.com  
555 Eleventh Street NW, Suite 1000  
Washington, D.C. 20004  
Telephone: 202.637.2200

Melanie M. Blunschi (SBN 234264)  
melanie.blunschi@lw.com  
Kristin Sheffield-Whitehead (SBN 304635)  
kristin.whitehead@lw.com  
505 Montgomery Street, Suite 2000  
San Francisco, CA 94111-6538  
Telephone: 415.395.5942

Michele D. Johnson (SBN 198298)  
michele.johnson@lw.com  
650 Town Center Drive, 20th Floor  
Costa Mesa, CA 92626  
Telephone: 714.540.1235

**GIBSON, DUNN & CRUTCHER LLP**

Elizabeth K. McCloskey (SBN 268184)  
EMcCloskey@gibsondunn.com  
Abigail A. Barrera (SBN 301746)  
ABarrera@gibsondunn.com  
One Embarcadero Center, Suite 2600

/s/Carol C. Villegas

Carol C. Villegas (pro hac vice)  
Michael P. Canty (pro hac vice)  
Jake Bissell-Linsk (pro hac vice)  
Danielle Izzo (pro hac vice)  
Gloria J. Medina (pro hac vice)  
**LABATON KELLER SUCHAROW LLP**

140 Broadway  
New York, NY 10005  
Telephone: (212) 907-0700  
Facsimile: (212) 818-0477  
cvillegas@labaton.com  
mcanty@labaton.com  
jbissell-linsk@labaton.com  
dizzo@labaton.com  
gmedina@labaton.com

*Co-Lead Class Counsel*

Christian Levis (pro hac vice)  
Amanda Fiorilla (pro hac vice)  
**LOWEY DANNENBERG, P.C.**  
44 South Broadway, Suite 1100  
White Plains, New York 10601  
Telephone: (914) 997-0500  
Facsimile: (914) 997-0035  
clevis@lowey.com  
afiorilla@lowey.com

*Co-Lead Class Counsel*

Diana J. Zinser (pro hac vice)  
Jeffrey L. Kodroff (pro hac vice)  
**SPECTOR ROSEMAN & KODROFF, P.C.**  
2001 Market Street, Suite 3420  
Philadelphia, PA 19103  
Telephone: (215) 496-0300  
Facsimile: (215) 496-6611  
dzinser@srkattorneys.com  
jkodroff@srkattorneys.com

*Co-Lead Class Counsel*

James M. Wagstaffe (SBN 95535)  
**ADAMSKI MOROSKI MADDEN  
CUMBERLAND & GREEN LLP**  
P.O. Box 3835  
San Luis Obispo, CA 93403-3835  
Tel: 805-543-0990  
Fax: 805-543-0980  
wagstaffe@ammcglaw.com

*Counsel for Plaintiffs Erica Frasco and*

1 San Francisco, CA 94111-3715  
2 Telephone: 415.393.8200

3 Christopher Chorba (SBN 216692)  
4 333 South Grand Avenue  
5 Los Angeles, CA 90071  
6 Telephone: 213.229.7503  
7 CChorba@gibsondunn.com

8 *Counsel for Defendant Meta Platforms, Inc.*  
9 *(formerly known as Facebook, Inc.)*

*Sarah Wellman*

Ronald A. Marron (SBN 175650)  
Alexis M. Wood (SBN 270200)  
Kas L. Gallucci (SBN 288709)  
**LAW OFFICES OF RONALD A.  
MARRON**  
651 Arroyo Drive  
San Diego, CA 92103  
Telephone: (619) 696-9006  
Facsimile: (619) 564-6665  
ron@consumersadvocates.com  
alexis@consumersadvocates.com  
kas@consumersadvocates.com

*Counsel for Plaintiffs Jennifer Chen and  
Tessa Gamino*

11 Kent Morgan Williams (*pro hac vice*)  
12 **SIRI GLIMSTAD LLP**  
13 745 Fifth Avenue, Suite 500  
14 New York, NY 10151  
15 Telephone: (929) 220-2759  
16 kent.williams@sirillp.com

17 William Darryl Harris, II (*pro hac vice*)  
18 **HARRIS LEGAL ADVISORS LLC**  
19 3136 Kingsdale Center, Suite 246  
20 Columbus, OH 43221  
21 Telephone: (614) 504-3350  
22 Facsimile: (614) 340-1940  
23 will@harrislegaladvisors.com

*Counsel for Plaintiffs Leah Ridgway and  
Autumn Meigs*